MMCS POLICY

FERPA and Confidentiality

FERPA

The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all educational agencies and institutions that receive funds under any program administered by the Department of Education. The law prohibits a school from disclosing personally identifiable information from students' education records without the consent of a parent or eligible student unless an exception to FERPA's general consent rule applies.

Moore Montessori Community School (MMCS) employees, contractors and volunteers are exposed to confidential information daily. Information concerning children and their families should be treated as confidential information, including personally identifiable information from students' education records. The School staff with access to this
information do not have the right to give this information to anyone who does not have a legitimate professional reason for access. Teachers or other staff members can be held liable for the individual release of information. Staff members are not permitted to discuss information about their students in open areas or where parents or other students have access. Anything said in meetings discussing students is considered confidential.

A student's name should not be in the subject box of an email. Their names should be treated as confidential as
well.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students." If you have questions regarding FERPA or have received a request for educational records, please contact the Head of School. See FERPA:

http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Confidentiality

Respecting the privacy of our students, donors, staff, and volunteers of the MMCS itself is a basic value of MMCS. Confidential information should not be disclosed or discussed with anyone without permission or authorization from the Head of School or Board of Directors. Care shall also be taken to ensure that unauthorized individuals do not overhear any discussion of confidential information and that documents containing confidential information are not left in the open or inadvertently shared.

Employees, volunteers and board members of MMCS may be exposed to information, which is confidential and/or privileged and proprietary in nature. It is the policy of MMCS that such information must be kept confidential both during and after employment or volunteer service. Staff and volunteers, including board members, are expected to return materials containing privileged or confidential information at the time of separation from employment or expiration of service. Unauthorized disclosure of confidential or privileged information is a serious violation of this policy and will

subject the person(s) who made the unauthorized disclosure to appropriate discipline, including removal/dismissal.

Handling and Transmitting Personally Identifiable Information
As a public school, MMCS frequently needs to share information from individual student records to resolve data issues and answer program area questions. Employees of the MMCS are legally and ethically obliged to safeguard the confidentiality of any private information they access while performing official duties. Private information regarding students and staff should always be transmitted securely.

FERPA is a federal law that applies to all educational agencies and institutions (e.g., schools) that receive funding under any program administered by the U.S. Department of Education. Among several purposes, FERPA was enacted to protect the privacy of students' educational records.

To the extent required by law, to protect the confidentiality of individuals from those who are not authorized to have access to individual-level data, Personally Identifiable Information (PII) will be encrypted during transmission using one of the following methods, in order of preference:

Secure FTP server based on SFTP or FTPS protocols.
Preferred method and most widely acceptable standard for transmitting encrypted data.

Encrypted Email
If secure FTP capabilities do not exist, encrypted email can be used.

Password Protected Email
If compatible encryption is not available to both parties, data should be password protected.

The password should be given to the recipient through a different medium, such as a phone call, never in notes or documents accompanying the actual data file, or another email. In addition, the password should not be transferred via voicemail.

When sending email, encrypted or password protected, MMCS will ensure that it contains the least amount of FERPA-protected information as possible. The subject line of an e-mail should not include FERPA-protected information; the body of an e-mail should not contain highly sensitive FERPA-protected information, such as a student's Social Security Number or full name. FERPA-protected data should always be in an attached encrypted/password protected file, never in the body of an email.

Fax machines and printers used to send and receive secure data must be located in areas that are secure.

Secure test questions, answer choices, or portions of secure test questions or answer choices must not be sent via e-mail (use e-mail only if encrypted and/or password protected).

The School does not use private or personal accounts to store students' personally identifiable information. To the extent that the School uses the G suite for Education (previously called Google Apps for Education), it will consult with their legal team to ensure compliance with FERPA and state security guidelines. Furthermore, the School will use the Data Leak Protection (DLP) feature of G Suite to protect data, even though FERPA compliance does not require DLP.

Protective Provisions and Maintenance of Student Records.
In addition, the School complies with all applicable state and federal law, including North Carolina General Statute Section 115C-400 et. seq. where applicable.

Internet Safety Policy

It is the policy of MMCS to:

(a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet,
electronic mail, or other forms of direct electronic communications;
(b) prevent unauthorized access and other unlawful online activity;
(c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors;
(d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Access to Inappropriate Material
To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage
To the extent practical, steps shall be taken to promote the safety and security of users of the online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes:
(a) unauthorized access, including so-called 'hacking,' and other unlawful activities; (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision and Monitoring
It shall be the responsibility of all members of the staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

MMCS provides Internet access to support education and research. Access to the Internet is a privilege subject to restrictions set by the Board of Directors. For students and staff, violation of any provisions in the Acceptable Use Policy (AUP) may result in disciplinary action and/or cancellation of access to the MMCS network. This policy applies to all Internet access on MMCS property, including Internet access using mobile devices, and including access by staff, students, and visitors to the MMCS campus.

Students' internet usage is permitted only in the presence and supervision of a teacher or other designated adult.
Although MMCS uses resources to protect against exposure to inappropriate material, there is always a risk of students accessing such materials. Although it may still be possible to access inappropriate material,

MMCS feels the educational benefit provided by the Internet outweighs any possible disadvantages. We encourage parents to talk with their students about sites and material which the parents believe are inappropriate. MMCS cannot accept responsibility for enforcing specific parental restrictions that go beyond those imposed by the school.

The Children's Internet Protection Act (CIPA) is a federal law enacted to address concerns about access to the Internet and other information. Under CIPA, schools must certify that they have certain Internet safety measures in place. These include measures to block or filter pictures that (a) are obscene, (b) contain child pornography, or (c) when computers with Internet access are used by minors, are harmful to minors. MMCS monitors online activities of minors to address (a) access by minors to inappropriate matter on the Internet and World Wide Web, (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications, (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online, (d) unauthorized disclosure, use, and dissemination of personal information regarding minors, and (e) restricting minors' access to harmful materials. MMCS certifies that it is in compliance with CIPA.

Students are prohibited from using or accessing Internet sites containing pornographic, violent or other unacceptable content either at school or at home using school-owned computers/technology/electronic devices. Accessing, producing, posting, displaying or sending offensive message, music or images, including images of exposed body parts is prohibited. Offensive material includes but is not limited to obscene, profane, lewd, vulgar, rude or sexually suggestive language or images.

Students who bring their own devices to campus are encouraged to take reasonable precautions to ensure the security of those devices. This includes operating system updates and virus scanning.

Safety and Ethical Use
Any internet user must take reasonable precautions to protect themselves online. Students, staff, and visitors should use the following guidelines:

Email, forums, instant messaging, and other online messaging
● Never share personal information online. This includes, but is not limited to: real full name, postal address, social security number, and passwords. Sharing the information of another individual, especially minors, is unethical, strictly forbidden, and may be unlawful. In the case of students, the privacy of student educational data is protected by the Family Educational Rights and Privacy Act (FERPA). When in doubt, do not release student data and consult a school administrator for further advice.
● Special care must be taken when sending mass emails. Email addresses themselves are private information, and improper mass emailing can result in inadvertent sharing of addresses. Improper mass emailing can also allow recipients to reply to the mass message and send their own messages to the entire group. This is preventable by using a blind carbon copy (Bcc) feature or a mass emailing service. It is the responsibility of all MMCS staff and students to use Bcc or a mass emailing service

and to protect private information and data when sending mass emails.

Unauthorized access / hacking and general unlawful activity

● Gaining or attempting to gain unauthorized access to MMCS resources, or using MMCS resources to gain or attempt to gain unauthorized access to outside systems is unethical, unlawful, and forbidden. This includes bypassing the internet filter without permission or purposefully gaining access to material that is harmful to minors.

● Assuming the online identity of another individual for any purpose is unethical and forbidden. ● Use of MMCS resources for any unlawful purpose, including, but not limited to, copyright infringement, is unethical and forbidden.

Academic integrity

● Students are expected to follow all Board and school handbook policies regarding academic integrity when using technology.

Harassment and Cyberbullying

Cyberbullying may involve any of these behaviors:

1. Accessing, producing, posting, sending, or displaying material that is offensive in nature on the internet 2. Harassing, insulting, or attacking others on the Internet

3. Posting personal or private information about other individuals on the Internet 4. Posting information on the Internet that could disrupt the school environment cause damage, or endanger students or staff

5. Concealing one's identity in any way, including the use of anonymization tools or another individual's credentials/online identity, to participate in any of the behaviors listed above.

The Head of School will determine whether or not specific incidents of cyberbullying have impacted the school's climate or the welfare of its students and appropriate consequences will be issued. MMCS is not responsible for electronic communication that originates off-campus but reserves the right, consistent with the law, to address conduct that occurs off school grounds where that conduct substantially disrupts the educational environment at MMCS or interferes with a student's learning at MMCS. Cyber bullying will be handled in accordance with Prohibition Against Discrimination, Harassment and Bullying Policy.